3. *Sung Y.-S.*, *Lee J.-H.*, *Kim Y.-H.* Optimal subcarrier pairing scheme for maximal ratio combining in OFDM power line communications // International Journal of Electronics and Communications (AEÜ). April, 2014. P. 1–6.

4. *Охрименко В.* PLC-технологии // Электронные компоненты. 2009. № 10. С. 58–62.

5. *Хорев А. А.* Средства перехвата информации с проводных линий связи. М., 2008. 24 с.

6. *Хорев А. А.* Организация защиты информации от утечки по техническим каналам. Информационная система «Техника для спецслужб» // Бюро научно-технической информации, 2000. 13 с.

7. *Götz M.*, *Rapp M.*, *Dostert K.* Power Line Channel Characteristics and Their Effect on Communication System Design // IEEE Communications Magazine. April, 2004. P. 78–86.

УДК 53083

Д. М. Кучин, Д. А. Паршин
Научный руководитель: доц. К. И. Костромитин
Южно-Уральский государственный университет, Челябинск

ПРИМЕНЕНИЕ МЕТОДОВ ДЕСТРУКТИВНОГО ТЕСТИРОВАНИЯ, РЕНТГЕНОВСКОГО И ЛОГИЧЕСКОГО АНАЛИЗА ДЛЯ АНАЛИЗА РАБОТЫ ИНТЕГРАЛЬНЫХ МИКРОСХЕМ

Аннотация. Представлены характеристики и описание методов обнаружения аппаратных закладок на основе методов деструктивного тестирования, оптических методов контроля, рентгеновского и логического анализа цепей интегральных микросхем.

Актуальность исследования рентгеновских методов анализа заключается в том, что данные методы являются базовыми и наиболее распространенными при проверке печатных плат на наличие сторонних включений. Актуальность применения метода логического анализа заключается в том, что он теоретически позволяет получить все множество значений сигналов, получаемых при работе интегральной микросхемы, что может быть использовано для аппаратной защиты информации

Ключевые слова: деструктивное тестирование; оптические методы контроля; рентгеновский анализ; логический анализ.

Метод деструктивного тестирования

Одним из постпроизводственных способов обнаружения аппаратных закладок является метод деструктивного тестирования. Его физический принцип заключается в последовательном удалении и фотографировании каждого из слоев чипа (в современных процессорах может быть более 10–15 слоев) и дальнейшем сравнении полученных фотографий с исходной маской процессора, по которой он изготавливался на фабрике. Метод характеризуется высокой трудоемкостью и позволяет с высокой степенью вероятности выявить лишние транзисторы и дорожки.

Рентгеновский метод анализа

Альтернатива деструктивному тестированию — это метод сканирования микросхемы рентгеновскими лучами, который позволяет добиться аналогичного эффекта без разрушения кристалла. Метод является проверкой того, что чип имеет только те функции, которые описаны документацией. Генерация рентгеновских лучей происходит за счет синхротрона, то есть ускорением электронов. При просвечивании различных компонентов цепи процессора, пучком рентгеновских лучей — медные провода, кремниевые транзисторы и другие детали рассеивают свет по-разному и вызывают конструктивную и деструктивную интерференцию. Направляя луч на образец под разными углами и используя технику, называемую рентгеновской птихографией (X-ray ptychography — сканирующая техника получения изображений объектов, размеры которых значительно превышают поперечные размеры фокального пятна (рентгеновского излучения, электронов) на образце [1]) (рис. 1), можно восстановить внутреннюю структуру чипа из полученных дифракционных картин [2].

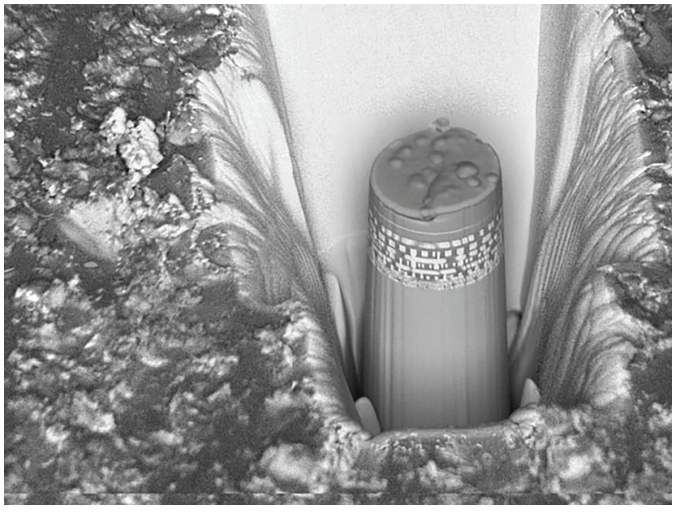

Рис. 1. Изображение внутренних разделов процессора Intel, полученное методом рентгеновской птихографии

Разрешение техники в одном из направлений составляет 14,6 нм, что создает довольно размытые изображения отдельных транзисторных компонентов. Образец должен оставаться стабильным, а интерферометры используются для постоянного измерения его положения. Требуется около 24 часов для проведения рентгеновских измерений, обработка данных занимает примерно столько же времени. При дальнейшем усовершенствовании источников рентгеновских лучей, а также других частей экспериментальной аппаратуры улучшится и скорость обработки изображений и разрешение метода.

Логический анализ

Имея свободный доступ к входам и выходам и набрав необходимую статистику отправленных и полученных сигналов, используя карту Карно, возможно извлечь внутреннюю логику (булевы функции) и восстановить алгоритм алгоритм работы интегральной микросхемы. Этот способ действенный, при наличии достаточных вычислительных мощностей и свободного доступа к системе. Сложность внутренней структуры микросхем, наличие в них последовательностных фрагментов и встроенных функций чрезвычайно затрудняют логический анализ проектов. Поэтому в настоящее время этот метод из-за сложности и размеров современных ПЛИС и реализуемых в них потоковых или блочных алгоритмов применяется для более простых схем, так как сложные схемы не поддаются логическому анализу.

Функция Readback. Специальная функция «readback» [3], предназначенная для чтения конфигурации схемы в целях облегчения отладки, предусматривается для большинства устройств типа FPGA. Злоумышленник может попробовать использовать ее через JTAG или интерфейс программирования. Ограничить доступ к конфигурации логики работы ПЛИС можно, используя биты безопасности. Но применение специальных регистров не гарантирует полной защищенности, так как, использовав аппаратные сбои и деактивировав биты безопасности, существует возможность получения доступа к конфигурации. Чаще уязвимость устраняют увеличением числа битов безопасности и встраиванием ПЛИС в надежную среду, в которой при обнаружении вмешательства вся конфигурация удаляется либо устройство самоуничтожается.

Для современных ПЛИС программирование производится непосредственно в составе системы без использования программатора (технология In-system programmability, ISP), на смонтированной плате, причем программирование ПЛИС может производится многократно. ПЛИС (например, микросхемы CPLD) программируются в системе через стандартный четырехконтактный JTAG интерфейс. Специальное ПО (Quartus II и др.) создает конфигурационную последовательность, которая загружается в ПЛИС с помощью специализированного загрузочного кабеля (XChecker для устройств фирмы Xilinx, ByteBlaster, BitBlaster или Master Blaster для устройств фирмы Altera).

Загрузочный конфигурационный кабель обеспечивает загрузку конфигурационных данных в микросхемы через стандартный последовательный порт PC или шину USB. Он обеспечивает конфигурирование микросхем с напряжениями питания 5,0; 3,3 и 2,5 Вольт; 1,8 В.

Для защиты прошивки ПЛИС от несанкционированного доступа большое распространение получило шифрование данных конфигурации. В таком случае на схему передается поток зашифрованных данных, который преобразуется в данные конфигурирования устройством дешифрации, находящимся на кристалле. Для этих целей используют генераторы и анализаторы Cyclic Redundance Code (CRC). Наиболее защищены от взлома схемы с пробиваемыми перемычками antifuse — однократно программируемые. Самыми уязвимыми считаются схемы с триггерной памятью конфигурации, которую нужно загружать от внешнего источника хранения данных при каждом включении питания.

Список литературы

1. Способы фокусировки рентгеновского излучения / Сторижко В. Е. и др. // Успехи физики металлов. 2010. С. 14.

2. *Courtland R.* 3D X-ray tech for easy reverse engineering of ICs [News] // IEEE Spectrum. 2017. Т. 54, № 5. P. 11–12.

3. Protecting against Cryptographic Trojans in FPGAs / Swierczynski P. et al. // Field-Programmable Custom Computing Machines (FCCM). 2015 IEEE23rd Annual International Symposium on // IEEE. 2015. P. 151–154.

УДК 53083

Р. И. Муталлапов, П. А. Моторин
Научный руководитель: доцент К. И. Костромитин
Южно-Уральский государственный университет, Челябинск

ПРИМЕНЕНИЕ МЕТОДОВ ИЗМЕРЕНИЯ ВОЛНОВОГО СОПРОТИВЛЕНИЯ, УЛЬТРАЗВУКОВЫХ ИЗМЕРЕНИЙ И ЭЛЕКТРОННОЙ МИКРОСКОПИИ ДЛЯ АНАЛИЗА РАБОТЫ ИНТЕГРАЛЬНЫХ МИКРОСХЕМ

Аннотация. Представлено описание и характеристики методов теплового, электрического, адаптерного и зондового контроля, применяемых для анализа функционирования интегральных микросхем.

Актуальность использования ультразвукового анализа обусловлена простотой и дешевизной применения данного метода, а метод электронной микроскопии по-